UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/942,010 | 08/29/2001 | Thomas S. Messerges | CR00286M | 9012 |

22917 7590 11/21/2006

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

| EXAMINER | |
|---|---|
| SHERKAT, AREZOO | |
| ART UNIT | PAPER NUMBER |
| 2131 | |

DATE MAILED: 11/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

## BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/942,010
Filing Date: August 29, 2001
Appellant(s): MESSERGES ET AL.

Lawrence J. Chapa
Reg. No. 39,135
For Appellant

## EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/21/2006appealing from the Office action mailed 10/19/2005.

### (1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

### (2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

### (3) Status of Claims

The statement of the status of claims contained in the brief is correct.

### (4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

### (5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

### (6) Grounds of Rejection to be Reviewed on Appeal

There are changes in the grounds of rejection as follow:

1. Claims 1-13, 15-32, 34-36, and 38-53 have been rejected under 35 U.S.C. 102(e) as being anticipated by Sweet et al., (U.S. Patent Publication No. 2002/0031230).

2. Claims 14, 33, and 37 are also rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (U.S. Patent Publication No. 2002/0031230).

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

| | | |
|---|---|---|
| 2002/0031230 | Sweet et al. | 3-2002 |

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

**NEW GROUND(S) OF REJECTION**

Claims 1-13, 15-32, 34-36, and 38-53 are rejected under 35 U.S.C. 102(e) as being anticipated by Sweet et al., (U.S. Patent Publication No. 2002/0031230 and Sweet hereinafter).

Regarding claim 1, Sweet discloses a communication device operable in a domain-based digital rights management environment (i.e., Constructive Key

Management (CKM) Architecture for Precise eXtensible Authentication, Authorization, and Administration (PXa^3))(page 4, par. 40-41), comprising:

a processing element (i.e., a desktop, a laptop, a mobile phone, or a PDA each have a processing element)(page 5, par. 80);

a receiver, coupled to and controlled by the processing element, operable to receive incoming messages to the communication device (i.e., the member's client system/device has a receiver because it is capable of downloading the soft token)(page 8, par. 116);

a transmitter, coupled to and controlled by the processing element, operable to transmit output messages of the communication device (i.e., client logs into the Pxa^3 and authenticate him or herself typically through user ID and password)(page 8, par. 116); and

a digital rights management module coupled to the processing element that controls operation of the communication device within the domain-based digital rights management environment (page 23-24, par. 386-387);

wherein the digital rights management module of the communication device in combination with a domain authority of the domain-based digital rights management environment is operable to selectively add the communication device to a domain having one or more communication devices (i.e., creating, administering, requesting, and distributing member profiles)(page 11, par. 149 and page 24, par. 392-394) that share a cryptographic key (i.e., the working key), which is associated with the domain (i.e., Domain value, shared by every one in the domain, is one of the three key values used to construct the working key)(page 9, par. 124-125), and thus permit the communication device to selectively receive and decrypt digital content based upon membership in the domain using the shared cryptographic key (page 9, par. 128).

Regarding claim 2, Sweet discloses the communication device of claim 1, wherein the transmitter is a limited range transmitter having a limited communication range and operable to transit the digital content to a trusted communication device within the limited communication range (i.e., it is inherent that the communication devices disclosed by Sweet, e.g., cellular phone, portable digital players, or wireless personal digital assistant are capable of transmitting in the limited communication range)(page 13, par. 173).

Regarding claims 3, Sweet discloses the communication device of claim 1, wherein in response to receiving a user request, the digital rights management module causes the transmitter of the communication device to transmit to a domain authority a request to register the communication device into the domain (page 24, par. 392-394), and wherein if the communication device is determined to have access to one or more valid cryptographic elements (i.e., domain value, maintenance value, and pseudo-random value), the digital rights management module causes the receiver of the communication device to receive over a communications channel the cryptographic key of the domain from the domain authority to link the communication device to the domain (i.e., creating the working key needed to decrypt the encrypted data object)(page 9, par. 128).

Regarding claim 4, Sweet discloses the communication device of claim 3, wherein the digital rights management module in combination with the domain authority removes the communication device from the domain, comprising:

in response to the request of the user of the domain to remove the communication device, the digital rights management module of the communication device causes the transmitter to transmit a request that the communication device be removed from the domain, in response to the request that the communication device be removed from the domain, the communication device receives from the domain authority via the secure communications channel a command to remove the cryptographic key of the domain from the communication device (i.e., once the decision to revoke is made, new encryption access denial should be as complete and rapid as security risks warrant)(page 12, par. 162), and upon receiving the command from the domain authority, the digital rights management module of the communication device removes the cryptographic key of the domain (i.e., updated maintenance values eliminate access to those members not in possession of the updated value. Maintenance value, updated by the domain authority, is one of the three key values used to construct the new working key)(page 9, par. 126 and pages 12-13, par. 165-167).

Regarding claim 5, Sweet discloses the communication device of claim 1, wherein in response to the digital rights management module of the communication device causing the transmitter to transmit a request for digital content, at least one of the digital rights management module of the communication device and the domain authority verifies authenticity of the domain (i.e., all members of the domain have been distributed the same domain value, which is one of the three values used to construct the working key; therefore, each time a member is provided with a working key to decrypt and view an encrypted data object, the authenticity of the domain is implicitly verified), and wherein upon verification of the authenticity of the domain, the receiver of the communication device receives an encrypted form of the requested digital content (i.e., encrypted data object) that is bound to the cryptographic key of the domain (i.e., the working key) in which the communication device is registered (page 9, par. 129 and page 10, par. 141-142).

Regarding claim 6, Sweet discloses the communication device of claim 1, wherein the digital rights management module of the communication device enforces usage rules associated with the requested digital content and received by the receiver in a content package containing the requested digital content (i.e., a pseudo-random value 215 is one of the key values necessary to make the working key 200, and the specific access permission credentials 225 are necessary to form the credential key 230. All credential categories included at the encryption of the information must be represented in the security profile 120 (FIG. 2) of anyone wishing to access that information, i.e., via decryption)(pages 9, par. 127-129 and page 11, par. 145).

Regarding claim 7, Sweet discloses the communication device of claim 6, wherein the content package comprises a binary representation rights table that contains the usage rules (page 10, par. 133).

Regarding claim 8, Sweet discloses the communication device of claim 7, wherein the binary representation rights table comprises a plurality of sections having predefined tokens (page 10, par. 133).

Regarding claim 9, Sweet discloses the communication device of claim 1, wherein the digital right management module, in response to the transmitter of the communication device receiving a request from a second communication device of the domain requesting the digital content, causes the transmitter to transmit the requested digital content from a storage element to the second communication device (page 9, par. 129 and page 10, par. 141-142).

Regarding claim 10, Sweet discloses the communication device of claim 1, wherein in response to a request of the user of the communication device, the digital rights management module causes the transmitter to transmit a request for digital content that is not available in the domain, and wherein after authenticity of the domain has been verified, the receiver receives an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered (i.e., establishing trust relationship between multiple domains, so that members of the second domain may use the imported credentials to share information with members of the first domain)(page 6, par. 88).

Regarding claim 11, Sweet discloses the communication device of claim 10, wherein the encrypted form of the requested digital content is contained in a content package (page 10, par. 134).

Regarding claim 12, Sweet discloses the communication device of claim 11, wherein the content package further comprises a binary representation rights table that contains the usage rules of the requested digital content (page 10, par. 133).

Regarding claim 13, Sweet discloses the communication device of claim 12, wherein the binary representation rights table comprises a plurality of sections having predefined tokens (page 10, par. 133).

Regarding claim 15, Sweet discloses the communication device of claim 10, wherein the digital rights management module of the communication device enforces usage rules associated with the requested digital content and received by the receiver in a content package containing the requested digital content (i.e., a pseudo-random value 215 is one of the key values necessary to make the working key 200, and the specific access permission credentials 225 are necessary to form the credential key 230. All credential categories included at the encryption of the information must be represented in the security profile 120 (FIG. 2) of anyone wishing to access that information, i.e., via decryption)(pages 9, par. 127-129 and page 11, par. 145).

Regarding claim 16, Sweet discloses the communication device of claim 15, wherein the content package comprises a binary representation rights table that contains the usage rules (page 10, par. 133).

Regarding claim 17, Sweet discloses the communication device of claim 16, wherein the binary representation rights table comprises a plurality of sections having predefined tokens (page 10, par. 133).

Regarding claim 18, Sweet discloses the communication device of claim 1, wherein in response to the receiver receiving a request from a second communication device of the one or more communication devices of the domain for the digital content and the digital rights management module verifying the authenticity of the second communication device (i.e., the consumer-member 105 would have a Pxa^3 member account 300 and appropriate credentials 115 for his section of the club, i.e., domain 100, along with downloaded Pxa^3 member client application software 850 for his "**player devices**")(page 13, par. 172), the digital rights management module causing the transmitter to transmit the requested digital content from a storage element of the communication device to the second communication device (i.e., downloading tracks into portable devices, e.g., a portable digital player, to and from the personal computer)(page 13, par. 173).

Regarding claim 19, Sweet discloses the communication device of claim 1, wherein the digital rights management module causes digital legacy content received from a source external (i.e., content vendor) to the domain to be stored in a storage element of the communication device (i.e., personal computer), and wherein in response to a request from a second communication device of the domain (i.e., a portable digital player), the digital rights management module causes the transmitter to transmit the digital legacy content from the storage element to the second communication device (page 13, par. 172-173).

Regarding claim 20, Sweet discloses a method of operation of a communication device of a domain having one or more communication devices that share a cryptographic key, which is associated with the domain and is used to decrypt select digital content, in a domain-based digital rights management environment, comprising:

in response to a user request, the communication device communicating to a domain authority a request to register the communication device into a domain; and

if the communication device is determined to have access to one or more valid cryptographic elements, the communication device receiving over a communications channel a cryptographic key of the domain from the domain authority that links the communication device to the domain.

Regarding claim 21, Sweet discloses the method of claim 20, further comprising:

the communication device, of a domain having one or more communication devices that share a cryptographic key of the domain, requesting digital content;

in response to the communication device requesting digital content, at least one of the communication device and the domain authority verifying authenticity of the domain; and

upon verification of the authenticity of the domain, the communication device receiving an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered.

Regarding claim 22, Sweet discloses the method of claim 21, further comprising the communication device enforcing usage rules associated with the requested digital content and received in a content package containing the requested digital content (page 10, par. 133).

Regarding claim 23, Sweet discloses the method of claim 22, wherein the content package comprises a binary representation rights table that contains the usage rules (page 10, par. 133).

Regarding claim 24, Sweet discloses the method of claim 23, wherein the binary representation rights table comprises a plurality of sections having predefined tokens (page 10, par. 133).

Regarding claim 25, Sweet discloses the method of claim 21, further comprising: a second communication device of the one or more communication devices of the domain requesting the digital content, and transferring the requested digital content from a storage element to the second communication device (i.e., the downloading device , e.g., personal computer, preferably has a large memory and a serial bus connection, e.g., a Universal Serial Bus cable, for downloading tracks into portable devices, e.g., a portable digital player, to and from the personal computer)(page 13, par. 173).

Regarding claim 26, Sweet discloses the method of claim 20, wherein removing the communication device from the domain comprises:

in response to the request of the user of the domain to remove the communication device, the communication device transmitting a request that the communication device be removed from the domain (i.e., once the decision to revoke is made, new encryption access denial should be as complete and rapid as security risks warrant)(page 12, par. 162); and

in response to the request that the communication device be removed from the domain, the communication device receiving from the domain authority via the secure communications channel a command to remove the cryptographic key of the domain from the communication device (i.e., updated maintenance values eliminate access to those members not in possession of the updated value. Maintenance value, updated by the domain authority, is one of the three key values used to construct the new working key)(page 9, par. 126 and pages 12-13, par. 165-167).

Regarding claim 27, Sweet discloses the method of claim 26, further comprising:

upon receiving the command from the domain authority, the communication device removing the cryptographic key of the domain (i.e., updated maintenance values eliminate access to those members not in possession of the updated value. Maintenance value, updated by the domain authority, is one of the three key values used to construct the new working key)(page 9, par. 126 and pages 12-13, par. 165-167).

Regarding claim 28, Sweet discloses the method of claim 20, wherein prior to the communication device communicating to a domain authority the request to register the communication device into the domain (i.e., retrieve member token request), further comprising the communication device:

communicating to the domain authority a request to establish the domain, said request having a domain name and a domain password (page 24, par. 392);

communicating to the domain authority via a communications channel a unique identifier of the communication device, downloading the cryptographic key created by the domain authority (page 24, par. 393-395).

Regarding claim 29, Sweet discloses the method of claim 20, further comprising:

in response to a request of the user of the communication device, the communication device requesting digital content that is not available in the domain, and after authenticity of the domain has been verified, the communication device receiving an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered (i.e., establishing trust relationship between multiple domains, so that members of the second domain may use the imported credentials to share information with members of the first domain)(page 6, par. 88).

Regarding claim 30, Sweet discloses the method of claim 29, wherein the encrypted form of the requested digital content is contained in a content package having usage rules enforced by the communication device (page 10, par. 133).

Regarding claim 31, Sweet discloses the method of claim 29, wherein the content package comprises a binary representation rights table that contains the usage rules (page 10, par. 133).

Regarding claim 32, Sweet discloses the method of claim 31, wherein the binary representation rights table comprises a plurality of sections having predefined tokens (page 10, par. 133).

Regarding claim 34, Sweet discloses the method of claim 29, further comprising:

the communication device receiving a request from a second communication device of the one or more communication devices of the domain requesting the digital content, the communication device verifying the authenticity of the second communication device (i.e., the consumer-member 105 would have a Pxa^3 member account 300 and appropriate credentials 115 for his section of the club, i.e., domain 100, along with downloaded Pxa^3 member client application software 850 for his "**player devices**")(page 13, par. 172); and

if the authenticity of the second communication device is verified, the communication device transferring the requested digital content from a storage element of the communication device to the second communication device (i.e., downloading tracks into portable devices, e.g., a portable digital player, to and from the personal computer)(page 13, par. 173).

Regarding claim 35, Sweet discloses the method of claim 20, further comprising:

the communication device receiving digital legacy content from a source external (i.e., content vendor) to the domain and storing it in a storage element of the communication device (i.e., personal computer), and in response to a request from a second communication device of the domain (i.e., portable digital player), the communication device transmitting the digital legacy content from the storage element to the second communication device (i.e., a portable digital player), the digital rights management module causes the transmitter to transmit the digital legacy content from the storage element to the second communication device (page 13, par. 172-173).

Regarding claims 36 and 39, Sweet discloses a method for registering devices in a domain having one or more communication devices that share a cryptographic key, which is associated with the domain and is used to decrypt select digital content, in a domain-based digital rights management environment, comprising:

a domain authority receiving a request to add a communication device to the domain (page 24, par. 392-394);

the domain authority determining whether the communication device is legitimate by verifying that the communication device has access to one or more valid cryptographic elements (i.e., domain value, maintenance value, and pseudo-random value), and if the communication device is determined to be valid, the domain authority transmitting over a communications channel to the communication device a cryptographic key of the domain operable to link the communication device to the domain (i.e., creating the working key necessary to decrypt the encrypted data object)(page 9, par. 128).

Regarding claim 38, Sweet discloses the communication device of claim 36, further comprising prior to receiving a request to add the communication device to the domain, the domain authority receiving a request to create the domain having a domain name and a domain password, the domain authority initiating the communications channel with the communication device, the domain authority determining a unique identification of the communication device, the domain authority establishing the domain using the unique identification of the communication device, the domain name, and the domain password (page 24, par. 392-395), the domain authority creating the cryptographic key of the domain, and the domain authority providing the cryptographic key for download by the communication device (page 9, par. 128 and par. 131).

Regarding claim 40, Sweet discloses the method of claim 36, wherein removing the communication device from the domain comprises the domain authority:

receiving the request to remove the communication device from the domain;

authenticating the communication device (i.e., once the decision to revoke is made, new encryption access denial should be as complete and rapid as security risks warrant)(page 12, par. 162), and upon authenticating the communication device the domain authority transmitting via a secure communications channel to the communication device a command to remove the cryptographic key of the domain from the communication device (i.e., updated maintenance values eliminate access to those members not in possession of the updated value)(page 9, par. 126 and page 12-13, par. 165-167).

Regarding claim 41, Sweet discloses the communication device of claim 36, further comprising the domain authority:

maintaining a log of requests by the communication device to register to or be deleted from one or more domains, monitoring the log to identify potentially fraudulent activity by the communication device, and generating a warning message in response to identifying potentially fraudulent activity by the communication device (i.e., monitoring/reporting/logging service module logs all meaningful events for billing, access control, and system monitoring use)(page 18, par. 284-291).

Regarding claim 42, Sweet discloses the method of claim 41, further comprising revoking a public key of the communication device if the communication device is determined to be engaged in fraudulent activity (i.e., eliminating undesirable members. It is also inherent that an eliminated member will lose Diffie-Hellman public key-based credentials and the corresponding private key-based credentials to be prevented from encrypting and decrypting data objects) (page 9, par. 126 and page 10, par. 133).

Regarding claim 43, Sweet discloses a domain-based digital rights management system, comprising:

a communication device linked via a first communications link to a domain-based digital rights management environment (i.e., CKM Architecture for Pxa^3)(page 4, par. 40-41), comprising:

a processing element (i.e., a desktop, a laptop, a mobile phone, or a PDA each have a processing element)(page 5, par. 80);

a receiver, coupled to and controlled by the processing element, operable to receive incoming messages to the communication device (i.e., the member's client system/device has a receiver because it is capable of downloading the soft token)(page 8, par. 116);

a transmitter, coupled to and controlled by the processing element, operable to transmit output messages of the communication device (i.e., client logs into the Pxa^3 and authenticate him or herself typically through user ID and password)(page 8, par. 116); and

a digital rights management module coupled to the processing element that controls operation of the communication device within the domain-based digital rights management environment (page 23-24, par. 386-387);

a domain authority coupled to the communication device via a second communications link, wherein the digital rights management module of the communication device in combination with the domain authority are operable to selectively add the communication device to a domain having one or more communication devices (i.e., creating, administering, requesting, and distributing member profiles corresponding to member devices)(page 11, par. 149 and page 24, par. 392-394) that share a cryptographic key (i.e., the working key), which is associated with the domain (i.e., Domain value, shared by every one in the domain, is one of the three key values used to construct the working key)(page 9, par. 124-125), and thus permit the communication device to selectively receive and decrypt digital content based upon membership in the domain using the shared cryptographic key (page 9, par. 128).

Regarding claim 44, Sweet discloses a method of limiting access to digital content in a domain-based digital rights management environment, comprising:

a first communication device, of a domain having one or more communication devices that share a cryptographic key of the domain, requesting digital content (page 9, par. 129);

in response to the request from the first communication device, verifying authenticity of the domain (i.e., all members of the domain have been distributed the same domain value, which is one of the three values used to construct the working key; therefore, each time a member is provided with a working key to decrypt and view an encrypted data object, the authenticity of the domain is implicitly verified), and upon verifying authenticity of the domain, making the requested digital content accessible to the first communication device by binding an encrypted form of the requested digital content to the cryptographic key of the domain to which the first communication device is registered (page 9, par. 124-129).

Regarding claim 45, Sweet discloses the method of claim 44, wherein the encrypted form of the requested digital content is contained in a content package having usage rules enforced by the first communication device (page 10, par. 133).

Regarding claim 46, Sweet discloses the method of claim 45, wherein the content package comprises a binary representation rights table that contains the usage rules (page 10, par. 133).

Regarding claim 47, Sweet discloses the method of claim 46, wherein the binary representation rights table comprises a plurality of sections having predefined tokens (page 10, par. 133).

Regarding claim 48, Sweet discloses the method of claim 44, wherein prior to the first communication device requesting digital content establishing the domain, said establishing further comprising:

in response to a user request, the first communication device communicating to a domain authority a request to register the first communication device into the domain (page 24, par. 392-394), the domain authority determining whether the first communication device is legitimate by verifying that the first communication device has access to one or more valid cryptographic elements (i.e., domain value, maintenance value, pseudo-random value), and the first communication device receiving over a communications link a cryptographic key of the domain from the domain authority that links the first communication device to the domain (i.e., creating the working key needed to decrypt the encrypted data object)(page 9, par. 128).

Regarding claim 49, Sweet discloses the method of claim 44, further comprising: a second communication device of the one or more communication devices of the domain requesting the digital content, and transferring the requested digital content from a storage element to the second communication device (i.e., the downloading device , e.g., personal computer, preferably has a large memory and a serial bus connection, e.g., a Universal Serial Bus cable, for downloading tracks into portable devices, e.g., a portable digital player, to and from the personal computer)(page 13, par. 173).

Regarding claim 50, Sweet discloses further comprising a second communication device of the one or more communication devices of the domain receiving digital legacy content from a source external (i.e., content vendor) to the domain and storing it in a storage element of the second communication device (i.e., personal computer), and in response to a request from a third communication device of the domain (i.e., portable digital player), the second communication device transmitting the digital legacy content from the storage element to the third communication device (page 13, par. 172-173).

Regarding claim 51, Sweet discloses the method of claim 44, further comprising removing a second communication device from the domain in response to a request from a user of the domain (page 12, par. 166).

Regarding claim 52, Sweet discloses the method of claim 51, wherein removing the second communication device from the domain comprises:

in response to the request of the user of the domain to remove the second communication device, the second communication device transmitting a request to the domain authority to remove the second communication device from the domain (page 12, par. 163-165);

in response to the request that the second communication device be removed from the domain, the domain authority transmitting a command via the secure communications channel to remove the cryptographic key of the domain from the second communication device, and upon receiving the command from the domain authority, the second communication device removing the cryptographic key of the domain resident on the second communication device (page 13, par. 166-167).

Regarding claim 53, Sweet discloses the method of claim 52, wherein the request that the second communication device be removed from the domain is made by the user at a website of the domain authority (i.e., member's access permissions are associated with client systems/devices – page 24, par. 394 - therefore, revocation of a member's access permissions is the same as removing the corresponding client device from the domain)(page 12, par. 166).

Claims 14, 33, and 37 are also rejected under 35 U.S.C. 103(a) as being unpatentable Sweet et al. (U.S. Patent Publication No. 2002/0031230).

Regarding claim 14, Sweet discloses the communication device of claim 10, wherein the member token file is encrypted, hashed and then stored in the member's client system. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use a non-volatile memory as an open-access storage (page 6, par. 81 and page 24, par. 389).

Regarding claim 33, Sweet discloses the communication device of claim 29, wherein the member token file is encrypted, hashed and then stored in the member's client system. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use a non-volatile memory as an open-access storage (page 6, par. 81 and page 24, par. 389).

Regarding claim 37, Sweet discloses the communication device of claim 36, wherein the Forward Maintenance Level (FML) of the Maintenance Value is used to deny a domain member access to CKM encrypted information beyond a specific point in time. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to determine that the one or more communication devices of the domain do not exceed a predetermined upper limit by denying a domain member access to CKM encrypted information beyond a specific point in time, e.g., the Forward Maintenance Level (FML) of the Maintenance Value (page 8, par. 119).

**(10) Response to Argument**

***A. Rejection under 35 U.S.C. 102***

Appellant argues that "the Examiner has failed to establish that any of the relied upon teachings from the reference are entitled to a date, which would establish the same as a prior teaching" (Appellant's Brief: page 6).

Examiner responds that Sweet et al. claims priority to provisional applications 60/225,796 and 60/239,019, which both support the relied upon features of U.S. Patent Publication 2002/0031230, at least to the extent set forth by the claimed invention in the instant application.

Appellant argues, "Sweet et al., does not provide for a cryptographic key, which is shared by the entities, which could be characterized as one or more communication devices, or which form a domain for accessing domain authorized content. Alternatively, Sweet et al., '230, includes a working key, which is generally unique for each data object including information of interest (see pg. 1, par. [0011]). Sweet et al., '230, in addition to including a working key, further includes credential keys, which may limit access to portions of a data object (see pg. 1, par. [0014]), dependent upon the set of credentials in a particular user's member profile, that is generally unique for each user (see pg. 3, par. [0035])" (Appeal Brief: page 7).

Examiner responds that the working key disclosed by Sweet et al., is constructed from three key values: **a domain value, which is shared by everyone in the domain** and provided by the security profile of the member account, a maintenance value, which is provided by the security profile of the member account, and **a pseudo-**

**random value, which is uniquely generated each time a data object is encrypted** and is transmitted and/or stored along with the encrypted data object 220 and as part of the CKM Header 235 (Figure 3)(page 9, par. 124-127). Therefore, as Appellant correctly points it out, the working key is infact unique for each data object due to the fact that it includes the unique pseudo-random value in it. It is also true that the system generates and securely transmits the working key over the public network; however, only the (domain) member's client system/application (on the client device) who have to the credentials key in the security profile in the system can access/decrypt the encrypted data object (page 9, par. 125 and par. 132 also page 11, par. 146-147).

To further segregate access to encrypted data objects, Sweet et al., further discloses categorizing different groups of authorized members and using Boolean function to define the access permission credentials 225 to form the credential key 230, necessary to decrypt the pseudo-random value which is in turn the third value used to create the working key 200. All credential categories included at the encryption of the information must be represented in the security profile 120 (FIG. 2) of anyone wishing to access that information (via decryption)(page 11, par. 145-147 – figure 3).

Appellant argues "At best, the encrypted data object, identified in the cited reference, and not the associated header file, is more closely akin to content. Consequently a domain level of access to a header file is not the same as providing a shared domain-level cryptographic key, which enables the receipt and decryption of digital content, based upon membership in the domain, as provided by the claims of the present application. "Content" is defined by the American Heritage Dictionary of the

English Language, Fourth Edition, published by the Houghton Mifflin Company (2000), as "the substantive or meaningful part". Alternatively, "header" is defined by the Free On-line Dictionary of Computing, Denis Howe, (1993-2004), as "the portion of a packet, preceding the actual data" and "the part of an electronic mail message or news article that precedes the body of a message". Hence, one skilled in the art would not recognize header information as being equivalent to content" (Remarks, page 7).

Examiner contends that Sweet et al., clearly discloses the encrypted data object 220 corresponding to the claimed digital content in the instant application (Figure 3). Sweet et al., further discloses a CKM Header 235 including the encrypted pseudo-random value 215, which is later decrypted with the proper credential key 230. Ultimately, the working key, constructed from domain, maintenance, and pseudo-random values, **is used to decrypt the encrypted data object 220**, which is different from the CKM Header file 235 (page 9, par. 128 and Figure 3).

Appellant argues that “Even at a more basic level, the use of the term domain in the cited reference relates to a group of members identified through individual member accounts, which is silent as to "having one or more communication devices", as provided by the claims of the present application. While the present application describes members as having individual member accounts and corresponding member tokens, no such designation is described relative to one or more various communication devices” (Remarks, page 8).

Examiner responds that Sweet et al., discloses that upon successful authentication of a member, PXa.sup.3 server system will download an encrypted ephemeral soft token to the member's client system (desktop, laptop, mobile phone, wireless personal digital assistant, etc.), which, after enrollment, will contain PXa.sup.3 client software. Once the soft token is safely deposited into the member's client system, the member may use the PXa.sup.3 system to encrypt or decrypt objects as he or she goes about his or her daily business (page 8, par. 116). Sweet et al., further discloses that during the "retrieve token request", a serial number uniquely identifying the member's client device and created during the member client package installation has to be sent to the Pxa^3 server system to retrieve the member's latest token from the Pxa^3 server system via the Internet (page 24, par. 391-394).

***B. Rejections under 35 U.S.C. 103***

Appellant's arguments, see Appeal Brief, page 10, filed 8/21/2006, with respect to the rejection(s) of claim(s) 14, 33, and 37 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Sweet et al., (U.S. Patent Publication 2002/0031230).

As per claims 14 and 33, the instant application discloses the communication device storing the encrypted digital content in an open-access storage element.

Sweet et al. Discloses wherein the member token file (i.e., the digital content) is encrypted, hashed and then stored in the member's client system (page 6, par. 81 and page 24, par. 389 – wherein the client systems storage is a non-volatile memory which is an open-access storage).

As per claim 37, the instant application discloses wherein prior to the domain authority transmitting the cryptographic key to the communication device further comprising: the domain authority determining that the one or more communication devices of the domain do not exceed a predetermined upper limit.

Sweet et al. discloses wherein the Forward Maintenance Level (FML) of the Maintenance Value is used to deny a domain member access to CKM encrypted information (i.e., cryptographic key) beyond a specific point in time (i.e., a predetermined upper limit). This time-based access control allows the domain authority to specify and limit exactly what information a domain member may be able currently to access (page 8, par. 119).

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment,

affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

**A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:**

JAMES DWYER, DIRECTOR
TECHNOLOGY CENTER 2100

Conferees:

Kim Vu

Christopher Revak

CHRISTOPHER REVAK
PRIMARY EXAMINER

Respectfully submitted,

A.S 11/7/2006 A.S